I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service on the date shown below with sufficient postage as First Class Mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Dated: May 14, 2007 Signature: Maureen DiVito
(Maureen Divito)

Docket No.: 0081004.00176US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	John BRAINARD et al.	Confirmation No.:	3025
Application No.:	10/010,769	Art Unit:	2131
Filed:	December 4, 2001	Examiner:	L. Chai
Title:	METHOD AND APPARATUS FOR PERFORMING ENHANCED TIME-BASED AUTHENTICATION		

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is RSA Security, Inc. of 174 Middlesex Turnpike, Bedford, Massachusetts 01730.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

On April 12, 2006, the Examiner issued a final rejection of all of the claims pending in this application (i.e., claims 1-31). On October 12, 2006, the appellants filed a Notice of Appeal appealing the Examiner's rejection of claims 1-31.

The claims on appeal are claims 1-31.

IV. STATUS OF AMENDMENTS

No proposed amendments were filed subsequent to receiving the final office action in this matter.

V. SUMMARY OF CLAIMED SUBJECT MATTER

As discussed in the Background of the Invention, methods for authenticating an identity of an entity are known that are based on something the entity knows or something the entity has, e.g. a biological characteristic of the entity or some combination of those things. One such computer-based authentication method involves the communication of ***a secret*** that is unique to a particular entity or user. The entity that is seeking authentication transmits the secret to a verifier who authenticates the identity of the entity. Typically, the entity communicates both identifying information (such as a user name) and the secret (such as a password) to the verifier. The verifier typically possesses records that associate a secret with each entity. If the verifier receives a secret that matches an appropriate record, the authentication of the entity is successful. If the verifier receives an incorrect secret, the authentication fails. (see ¶ [0002])

Time-based authentication systems also associate an entity with a secret, typically a number, which is unique to that entity. These systems generally perform some algorithmic processing of the secret to generate an ***authentication code*** that is ultimately used to authenticate the entity. Some time-based systems use a dynamic variable to calculate a non-predictable authorization code that ultimately authenticates the entity. Here, "non-predictable" means that the authorization code is not predictable by a party that does not know the associated secret, the algorithm for calculating the code, or both. The dynamic variable may comprise any code, typically a number, which is defined and determined by the interval of time in which an authentication code is generated. The dynamic variable typically changes according to an interval of time, e.g., 2 minutes, 5 minutes, 1 hour or whatever. Because in these systems the authentication code changes from time to time, intercepted authentication information has a limited value because it cannot be used for authentication in the future during a different time interval. (see ¶ [0003])

The user of such a system might employ a device to algorithmically compute the correct authentication code for a particular time interval. A typical device might be a hardware token

that is loaded with a program for carrying out the predetermined algorithm. The token might also allow the user to input a second, personally selected secret, such as a personal identification number (PIN) in order to generate a correct authentication code. In that case, only a correctly entered PIN produces a correct authentication code for a particular time interval. Such devices might display the generated authentication code to the user, who then communicates that authentication code to the verifier. (see ¶ [0004])

But even time-based authentication systems are vulnerable to attacks by third parties during the time interval during which the dynamic variable is valid. The third party attacker could enter multiple guesses for the personally selected secret values during an authentication time period. By associating each personally selected secret with the resulting authentication code generated by the device, a sophisticated attacker could mathematically solve or otherwise determine the personally selected secret. A similar problem could occur if the user mistakenly provides one or more incorrect secret values and communicates one or more incorrect authentication codes on an insecure channel before communicating a correct authentication code generated from a correct secret value. An eavesdropping attacker can obtain sufficient information from these exchanges to mathematically solve for or otherwise determine the personally selected secret. (see ¶ [0005])

"The invention relates to computer-based methods and systems for time-based authentication that offer increased resistance to attack ***by generating different dynamic authentication codes within a single time interval***. Each authentication code is generated using a *generation value*, which is different for generation attempts within a time interval. In one embodiment, a combination function is employed that takes as input ***a secret***, ***a dynamic value***, ***a PIN value***, and ***a generation value***. (The combination function may also [include a] verifier identifier as well as other information.) ***Each authentication attempt during the same time interval uses a different generation value and, in some embodiments, the receipt of the PIN triggers a change in the generation value***. Use of this generation value in the combination function makes it more difficult for an attacker to attack the system by generating or observing the generation of multiple authentication codes within a timer interval, because information that previously was available to the attacker in the prior art systems is now hidden." (see ¶ [0006])

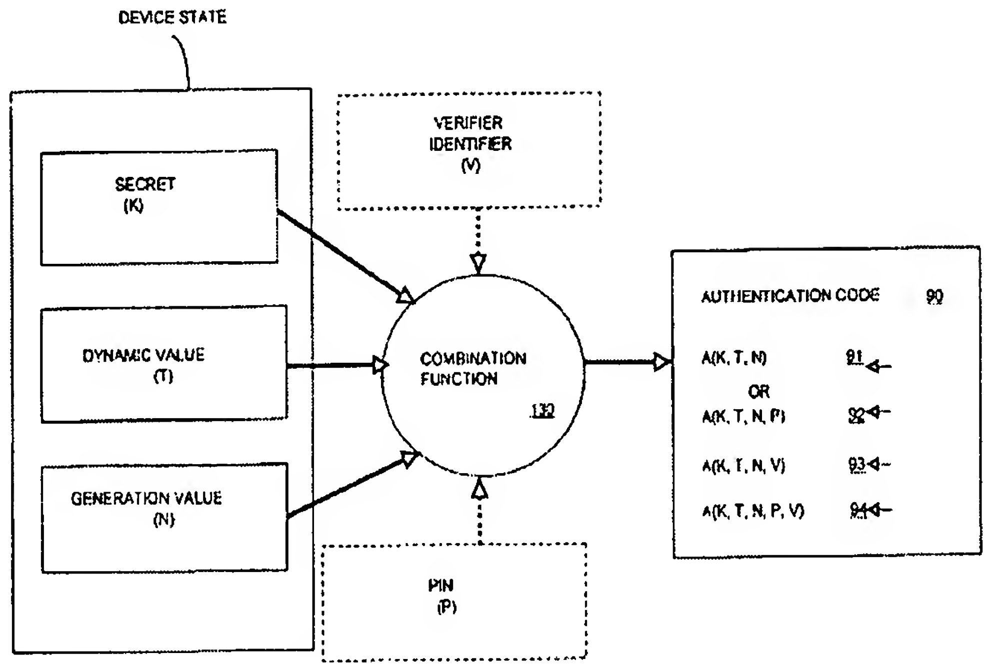

FIG. 2

FIG. 2 depicts one embodiment of the user authentication device in which various values are combined by a combination function 130 to generate an authentication code 90. In general, the combination function 130 generates an authentication code 90 using the state of the user authentication device 120. FIG. 2 shows, as examples of device state that may be used, the secret (K) stored by the user authentication device 120, a dynamic, time-varying value (T) generated by the user authentication device 120, and a generation value (N), which will be discussed in greater detail below. Other examples of device state include the time and date of manufacture of the user authentication device 120, the amount of time since generation of the last authentication code, an encoding of the latitude and longitude of the location of manufacture of the user authentication device 120, an encoding of the location of the user authentication device 120 at the time of generation of the user authentication device (using GPS or enhanced GPS, for example), or other similar quantities. (see ¶ [0030])

The combination function 130 may also optionally use user state (shown in phantom view in FIG. 2 as PIN (P)) or verifier states (shown in phantom view in FIG. 2 as verifier identifier (V)) to generate an authentication code (A) 90 for the user. Other examples of user state include biometric information such as retinal scans and fingerprints, and identifying information such as social security number, birthdate (possibly including time of birth) or employee codes. Verifier state may include information identifying the verification computer 150, such as IP address or processor serial number. (see ¶ [0030])

Claim 1 is directed to combining a stored secret, a dynamic value associated with a time interval, a first generation value indicative of a number of previous authentication code generations, and a personal identification number (PIN) to generate an authentication code and generating a second generation value responsive to receipt of the PIN.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner rejected claims 1-28 and 30-31 under 35 U.S.C. § 103(a) as being unpatentable over Weiss (U.S. 4,884,778) in view of Kocher (U.S. 6,539,092). The Examiner explicitly admits that "Weiss does not disclose expressly retrieving a first generation value indicative of a number of previous authentication code generations;" and the Examiner also implicitly acknowledges that Weiss does not teach "generating a second generation value responsive to receipt of the PIN." For the missing elements he relies on Kocher.

The question for this appeal is whether Kocher by itself or in combination with the other references relied on by the Examiner teaches or suggests "generating a second generation value responsive to receipt of the PIN," as required by the claims.

VII. ARGUMENT

Claim 1: The combination of Weiss and Kocher does not teach or suggest generating a second generation value responsive to receipt of the PIN.

There is a fundamental difference between the subject of the present application and what is taught by Kocher. According to the present application, a primary goal of the described embodiment is to offer, in a system that uses a dynamic variable such as a time-based variable, increased resistance to an attack on the security of that system. That is, to make it more difficult for a third party to discover the secret that is required to authenticate a user within the system. This is accomplished by forcing a change in the computed authentication code after each attempt at gaining access within a given time interval. Towards this end, the claims explicitly recite generating a second generation value responsive to receipt of the PIN.

In contrast, Kocher wants his key to be used to complete a transaction and then require a new key for the next transaction. He accomplishes this by updating his counter upon completion

of a transaction and not upon the entry of the PIN as is required by the claims. This is clear from following passages that have been excerpted from Kocher:

> FIG. 1 shows an exemplary sequence of client device secret state values usable to perform a series of transactions, typically (but not necessarily) using one state per transaction. (Col. 3, lines 61-64). [emphasis added]
>
> As the states are updated, counter C is also updated (by one for each update). (Col. 4, lines 33-34). [emphasis added]
>
> **At step 110**, the device performs the first transaction, using K_C (or a key derived from K_C). The key can be used in virtually any symmetric cryptographic transaction. (For example, such a transaction could involve, without limitation, computing or verifying a MAC (Message Authentication Code) on a message, encrypting or decrypting a message, producing a pseudorandom challenge value, deriving a key, etc. Examples of messages include, without limitation, data specifying the amounts of funds transfer operations, e-mail messages, challenge/response authentication data, parameter update authorizations, code updates, audio messages, digitized images, etc.)
>
> **After step 110**, the client device's secret value K_C is updated by applying the function F_A and the counter C is incremented, i.e. by performing $C \leftarrow C+1$ and $K_C \leftarrow F_A(K_C)$. (Col. 4, lines 39-54). [emphasis added]

In other words, in Kocher's system the transaction is first completed or conducted (see step 110) and after that, the counter is incremented so that a new key will be used/required for the next transaction.

If one were to employ Kocher's mechanism in Weiss' system, the result would not be the claimed invention. That is, it would not be a system which operates by "generating a second generation value responsive to receipt of the PIN."

This might seem like a minor difference but in fact it is quite significant. A system that implemented Kocher's mechanism would not work as Kocher intended if it incremented the counter in response to receipt of the PIN. This fact can be appreciated by walking through a typical scenario.

Assume that a user of a system (i.e., Weiss' system modified by Kocher, as proposed by the Examiner) wants to conduct a transaction with the server. In that case, the client will receive the user's PIN, compute a key, and then use the computed key to authenticate to the server and conduct the transaction. But assume that the first attempt to conduct the transaction fails because, for example, the system does not succeed in establishing a connection with the server

or the transmission is corrupted. If the client increments the counter before the next attempt to conduct the transaction, e.g. in response to receipt of the user's PIN, then the next time the client generates a key for that transaction, its value will be different from the one that is being expected by the server. The server would not be aware of the change in the counter value and would use the last counter value. As a consequence, on this second attempt the next authentication key that is provided by the user within that time period would be different from the one that is expected and authentication would again fail. Indeed, it is hard to imagine how the client and the server would again achieve synchronization using only Kocher's algorithm if the client increments the counter in response to receipt of the PIN.

In short, the object of Kocher's system is to generate a key that can be used for a single transaction and then change it for the next transaction. If Kocher changes the key before a transaction is actually successfully completed, then the client and the server will get out of synch and the client will be unable to authenticate to the server. For the Kocher mechanism to operate properly, at least until the transaction has been completed, the key that it computes must be the same regardless of how many times that key is computed (for the same time interval).

There is no motivation or suggestion to be found in either reference to modify the way in which Kocher increments his counter. Indeed, Kocher's patent actually teaches away from modifying the counter in response to receipt of the PIN, as opposed to incrementing it in response to completion of the transaction.

Claim 17:

Claim 17 includes a limitation that is similar to limitation that is found in claim 1 and that was the subject of the discussion above. More specifically, it recites:

> a first generation value subsystem determining a first generation value indicative of a number of previous authentication code generations within the time interval and **calculating a second generation value responsive to receipt of the PIN** by the PIN subsystem

Thus, for the reasons present above in connection with claim 1, we submit that claim 17 is also patentable over the references relied on by the Examiner.

VIII. CLAIMS

A copy of the claims involved in the present appeal (i.e., claims 1-31) is attached hereto as Appendix A.

Respectfully submitted,

Dated: May 14, 2007

Eric L. Prahl
Registration No.: 32,590
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)

APPENDIX A

1. A method for generating an authentication code associated with an entity, the method comprising the steps of:

retrieving a stored secret associated with an entity;

determining a dynamic value associated with a time interval;

retrieving a first generation value indicative of a number of previous authentication code generations;

receiving a personal identification number (PIN);

generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN; and

generating a second generation value responsive to receipt of the PIN.

2. The method of claim 1 further comprising the step of receiving verifier information, and wherein the generating step comprises combining the stored secret, the dynamic value, the first generation value, the PIN, and the verifier information.

3. The method of claim 2 wherein the step of generating the authentication code comprises:

combining the stored secret and the dynamic value to form a first result;

combining the verifier information with the first result to form a second result; and

combining the first generation value with the second result.

4. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the PIN to form a first result;

combining the dynamic value with the first result to form a second result; and

combining the first generation value with the second result.

5. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the first generation value to form a first result;

combining the dynamic value with the first result to form a second result; and

combining the PIN with the second result.

6. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the dynamic value to form a first result; and

combining the first generation value with the first result.

7. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the stored secret and the first generation value to form a first result; and

combining the dynamic value with the first result.

8. The method of claim 1 wherein the step of generating the authentication code comprises:

combining the dynamic value and the first generation value to form a first result; and

combining the stored secret with the first result.

9. The method of claim 1 wherein the step of determining the dynamic value comprises determining a dynamic value responsive to a time-based counter.

10. The method of claim 1 wherein the step of determining a generation value comprises incrementing a generation counter for an authentication code generated during the time interval.

11. The method of claim 10, further comprising the step of resetting the generation counter at the start of a second time interval.

12. The method of claim 1 further comprising the step of the displaying the authentication code on a display.

13. The method of claim 1, wherein the PIN is retrieved from a data store.

14. The method of claim 1, further comprising the step of selecting a combination function based on the first generation value.

15. The method of claim 1, wherein the step of retrieving a stored secret comprises retrieving one of a plurality of stored secrets based on the first generation value.

16. The method of claim 1, wherein the step of retrieving a generation value comprises retrieving a first generation value indicative of a number of previous code generations within the time interval.

17. A system for generating an authentication code associated with an entity, the system comprising:

a memory element storing a secret associated with an entity;

a dynamic value subsystem determining a dynamic value associated with a time interval;

a personal identification number (PIN) subsystem receiving a PIN;

a first generation value subsystem determining a first generation value indicative of a number of previous authentication code generations within the time interval and calculating a second generation value responsive to receipt of the PIN by the PIN subsystem; and

a combination subsystem generating an authentication code by retrieving the secret from the memory element and combining the secret with the dynamic value from the dynamic value subsystem, the PIN received by the PIN subsystem, and the generation value from the generation value subsystem.

18. The system of claim 17 wherein the PIN subsystem further comprises a keypad.

19. The system of claim 17 wherein the combination subsystem combines the stored secret and the dynamic value to form a first result, combines the PIN with the first result to form a second result, and combines the first generation value with the second result.

20. The system of claim 17 wherein the combination subsystem combines the stored secret and the PIN to form a first result, combines the dynamic value with the first result to form a second result, and combines the first generation value with the second result.

21. The system of claim 17 wherein the combination subsystem combines the stored secret and the first generation value to form a first result, combines the dynamic value with the first result to form a second result, and combines the PIN with the second result.

22. The system of claim 17 wherein the combination subsystem combines the stored secret and the dynamic value to form a first result, and combines the first generation value with the first result.

23. The system of claim 17 wherein the combination subsystem combines the stored secret and the first generation value to form a first result, and combines the dynamic value with the first result.

24. The system of claim 17 wherein the combination subsystem combines the dynamic value and the first generation value to form a first result, and combines the stored secret with the first result.

25. The system of claim 17 wherein the dynamic value subsystem comprises a time-based counter, and the dynamic value subsystem determines a dynamic value responsive to the counter.

26. The system of claim 17 wherein the generation value subsystem comprises a generation counter that is incremented for each generation of the authentication code during the time interval.

27. The system of claim 26, wherein the generation value subsystem resets the generation counter at the start of a second time interval.

28. The system of claim 17 further comprising a display for displaying the generated authentication code.

29. The system of claim 17 wherein the generation value subsystem changes the generation value upon activation of a button.

30. The system of claim 17 wherein the PIN subsystem further comprises a data store for storing the PIN associated with a user.

31. The system of claim 17 wherein the first generation value subsystem determines a first generation value indicative of a number of previous authentication code generations within the time interval.